GRS: The Green, Reliability, and Security of Emerging Machine to Machine Communications

Rongxing Lu, Xu Li, Xiaohui Liang, and Xuemin (Sherman) Shen, University of Waterloo
Xiaodong Lin, University of Ontario Institute of Technology

ABSTRACT

Machine-to-machine communications is characterized by involving a large number of intelligent machines sharing information and making collaborative decisions without direct human intervention. Due to its potential to support a large number of ubiquitous characteristics and achieving better cost efficiency, M2M communications has quickly become a market-changing force for a wide variety of real-time monitoring applications, such as remote e-healthcare, smart homes, environmental monitoring, and industrial automation. However, the flourishing of M2M communications still hinges on fully understanding and managing the existing challenges: energy efficiency (green), reliability, and security (GRS). Without guaranteed GRS, M2M communications cannot be widely accepted as a promising communication paradigm. In this article, we explore the emerging M2M communications in terms of the potential GRS issues, and aim to promote an energy-efficient, reliable, and secure M2M communications environment. Specifically, we first formalize M2M communications architecture to incorporate three domains — the M2M, network, and application domains — and accordingly define GRS requirements in a systematic manner. We then introduce a number of GRS enabling techniques by exploring activity scheduling, redundancy utilization, and cooperative security mechanisms. These techniques hold promise in propelling the development and deployment of M2M communications applications.

INTRODUCTION

The exponential growth of wireless communication devices and the ubiquity of wireless communication networks have recently led to the emergence of wireless machine-to-machine (M2M) communications as the most promising solution for revolutionizing the future "intelligent" pervasive applications. The primary advantage of M2M communications is that many intelligent wireless devices may act as "servers," collaboratively collecting and delivering real-time monitoring data to people. Since it does not need direct human intervention, M2M communications is fast becoming a market-changing force for the next-generation intelligent real-time networked applications [1]. Currently, the best known application of M2M communications is probably the satellite navigation system, as shown in Fig. 1, which enables the transferring of up-to-date traffic information and relevant useful location information to drivers on the road. In the near future, M2M communications can be used to more efficiently monitor the conditions of patients, environmental resources, and so on. Foreseeably, as shown in Table 1, many promising real-time monitoring applications including e-healthcare, smart homes, environmental monitoring, and industrial automation can be revolutionized by the emerging M2M communications.

Despite the promising real-time monitoring applications and tremendous benefits, M2M communications is still in its infancy and faces many technical challenges. These challenges include M2M deployment architecture, M2M software, and M2M communication's energy efficiency, reliability, and security [2]. Recently, much attention has been paid to the deployment of architecture and software challenges in M2M communications not only from the IT industry but also from academia [2]. However, the energy efficiency, reliability, and security issues in M2M communications have not been well explored. According to a recent report on global carbon emissions [3], information and communication technology (ICT) accounts for 2–2.5 percent of all harmful emissions, which is almost equal to the global aviation industry. Therefore, to protect global environments, green communication has been widely advocated for achieving energy efficiency in communication networks. As a pervasive ICT, M2M communications, which encompasses a mass of intelligent wireless devices, obviously should satisfy the energy effi-

0163-6804/11/$25.00 © 2011 IEEE

ciency (green) requirement. Thus, not only is the global environment protected, but also the lifetime of M2M communications can be prolonged. In addition to the green requirement, M2M communications should also satisfy the reliability and security requirements, both of which are critical to the quality of service (QoS) provided by M2M communications. Clearly, if neither reliability nor security is guaranteed in M2M communications, there will be less interest in this newly emerging communication paradigm. Therefore, green, reliability, and security (GRS) requirements are essential to the success of M2M communications.

In this article, we technically discuss the energy efficiency, reliability, and security issues in emerging M2M communications, aiming to provide an energy-efficient, reliable, and secure M2M communications environment. We first give a high-level overview of M2M communications architecture and its GRS requirements. Then we address energy efficiency in M2M communications by introducing an efficient activity scheduling scheme [4] for energy saving. We also study reliability and security in M2M communications, and discuss several approaches to offer a reliable and secure M2M communications paradigm. Lastly, we provide conclusions on M2M communications with guaranteed GRS and the potential research issues.

Overview of M2M Communications Architecture and GRS Requirements

In this section, we formalize the M2M communications architecture and identify the GRS requirements.

M2M Communications Architecture

Figure 2a shows a high-level architecture of the emerging M2M communications paradigm, which mainly consists of three interlinked domains: the M2M, network, and application domains.

M2M domain: In the M2M domain, an M2M area network is potentially formed by a large number of M2M nodes $\{N_0, N_1, \cdots\}$ and an M2M gateway (GW). Each M2M node N_i is a very flexible and smart device equipped with some specific sensing technology (i.e., body sensors in an e-healthcare system or other types of sensors in environmental surveillance) for real-time monitoring. Once monitoring data are sensed, M2M nodes will make intelligent decision and transmit the sensory data packets to the GW in single-hop or multihop patterns. The M2M gateway GW is an integrated device. After collecting the packets from M2M nodes, it is able to intelligently manage the packets and provide efficient paths for forwarding these packets to the remote back-end server (BS) via wired/wireless networks, as shown in Fig. 2a.

Network domain: In the network domain, the great success of wired networks and the ubiquity of wireless networks (e.g., 3G cellular , WiMAX, and municipal Wi-Fi) provide cost-effective and reliable channels for transmitting the sensory data packets from the M2M domain to the application domain.

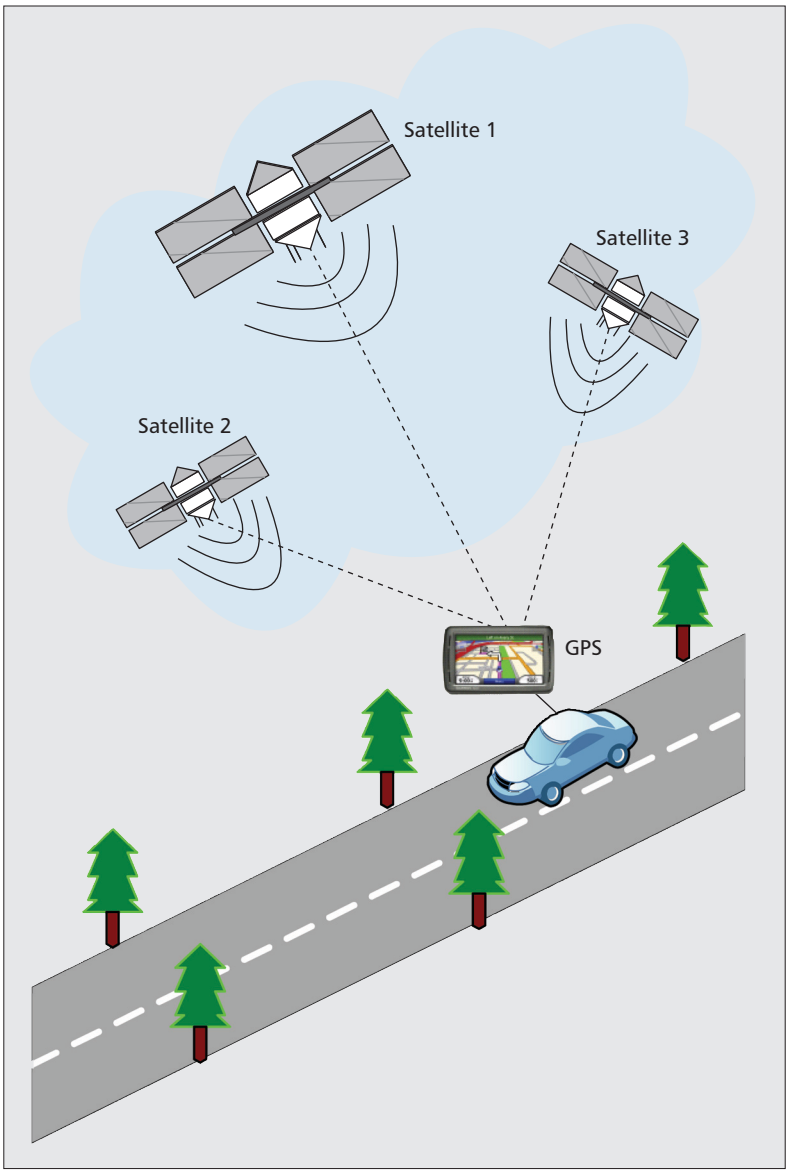

Figure 1. *Satellite navigation system, one of the best-known examples of M2M communications.*

Application domain: In the application domain, the BS is the key component for the whole M2M communications paradigm, which not only forms the data integration point for storing all sensory data from the M2M domain, but also provides these real-time data to a variety of M2M applications for remote monitoring management.

The GRS Requirements in M2M Communication

Although many current and rapidly growing M2M communications systems may have unique features, most M2M communications systems are generally organized in a similar architecture to that shown in Fig. 2a, with the following common characteristic: *a massive number of M2M nodes are deployed in the M2M domain to collect*

Typical applications	Benefits
E-healthcare	Remote patient monitoring for better healthcare
Smart home	Real-time remote security and surveillance
Environmental monitoring	Effective monitoring at low cost
Industrial automation	Remote equipment management for cost savings

Table 1. *Typical applications and benefits of M2M communications.*

useful monitoring data by sensing technologies and real-time processes, and transmit sensory data to the BS in the application domain without direct human intervention. This characteristic can benefit users from fast growing M2M communications in many promising applications; however, it also brings new GRS challenges. To successfully deploy M2M communications systems for next-generation real-time monitoring applications, the GRS requirements, as shown in Fig. 2b, must be satisfied.

Green: Since a mass of M2M nodes $\{N_0, N_1, \cdots\}$ are deployed in the M2M domain, M2M communications should focus on energy saving by optimizing M2M nodes' sensing, processing, and transmissions, and ultimately prolong the lifetime of the whole M2M communications. In addition, since the BS is also a power-consuming component in M2M communications, great efforts should also be made on the BS to achieve environmentally friendly, green M2M communications.

Reliability: Reliability is critical for green M2M communications, because unreliable sensing, processing, and transmission can cause false monitoring data reports, long delays, and even data loss, which would reduce people's interest in M2M communications. Therefore, the rapid growth of M2M communications demand of high-reliability.

Security: Security is also of utmost importance for M2M communications, especially for green M2M communications. The reasons are twofold. On one hand, the unattended M2M domain in many M2M applications makes an attacker able to easily launch some physical attacks, compromising M2M nodes; on the other hand, for energy saving, a fraction of M2M nodes could switch into sleeping mode, which further makes these attacks undetectable.

Generally speaking, energy efficiency, reliability, and security may easily be fulfilled individually in M2M communications. However, when GRS requirements are considered as a whole, the issues become complicated. In the following, we discuss the GRS issues in M2M communications by surveying several potentially useful solutions to shed light on this research line.

Energy Efficiency in M2M Communications

M2M communications are dependent upon the massive M2M nodes to intelligently collect monitoring data in M2M domain, the wired/wireless network to relay the collected sensory data to the BS in network domain, and the BS to support various M2M applications over network in application domain. Because a massive number of machines are involved in M2M communications, the energy efficiency (green) becomes a challenging issue especially in M2M domain. Communication dominates energy consumption, and energy efficiency can be increased by wisely adjusting transmission power (to the minimal necessary level), and carefully applying algorithmic and distributed computing techniques to design efficient communication protocols (e.g., routing protocols [5]). It can be further improved by activity

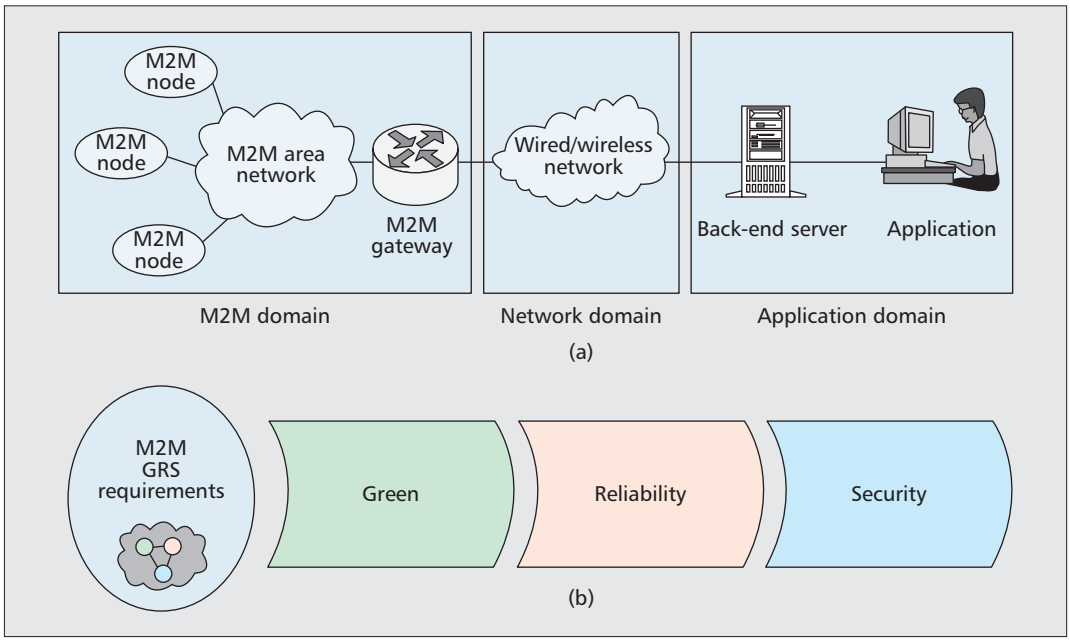

Figure 2. *M2M communications: a) architecture; b) GRS requirements.*

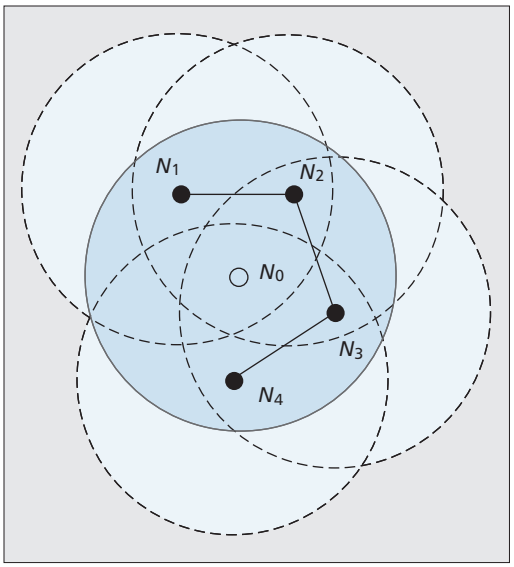

Figure 3. *An example that node* N_0 *may switch to sleep mode because its sensing range is fully covered by the connected neighbors* $N_1, \ldots, N_4$.

scheduling, the objective of which is to switch some nodes to low-power operation ("sleeping") mode so that only a subset of connected nodes remain active while the functionality (e.g., sensing and data gathering) of the original network is preserved.

In [4], an activity scheduling scheme is proposed for sensing coverage, which appears to be the best in the literature. This scheme requires time to be slotted, and activity scheduling is then done in rounds. In each round, a node selects a random timeout and listens to messages from neighbors before it expires. These messages contain the activity decision (i.e., whether to be active or not) of their senders. When the timeout expires, solely based on the received information, the node makes its own activity decision and announces it to neighbors by transmitting a message. A node decides to be active if its sensing range (coverage circle) is fully covered by the sensing ranges of a connected set of active neighbors.

The decision on full coverage is in turn grounded on a well-known geometric theorem (illustrated in Fig. 3, together with the connectivity consideration): if there are at least two coverage circles, and any intersection point of the two circles inside the sensing area is covered by a third coverage circle, the sensing area is fully covered. Some nodes may have announced themselves as active, and later, after receiving new announcements from neighbors, find that they are fully covered. In this case, they may change their previous decisions and enter sleep mode after announcing their new decisions. The scheme involves local communication only and generates a very small number of control messages, thus being energy efficient. Simulations based on ideal and realistic physical layers reveal its advantages over other similar algorithms. Therefore, the scheme can be applied to achieve green communications in the M2M domain.

Reliability in M2M Communications

For achieving green M2M communications, since not all M2M nodes are expected to simultaneously be active in the M2M domain, reliability is a challenging issue. In order to improve the reliability of M2M communications, exploiting redundancy technologies, including information redundancy, spatial redundancy, and temporal redundancy, can be an efficient approach for M2M communications. In the following, we discuss three major reliability issues in M2M communications with different redundancy technologies.

Reliability in Sensing and Processing

Due to component faults and so on, a single M2M node may not be sufficient to accurately sense and process monitoring data. Therefore, a majority vote in green M2M communications is desirable to improve reliability. In [6], a local vote decision fusion (LVDF) algorithm is presented, which can be directly applied in M2M communications. In LVDF, each M2M node N_i first independently senses, processes, and makes an initial single-bit decision $d_i \in \{0, 1\}$ on some event in a specific M2M application, and shares the decision d_i with its neighbors $NB(i)$. Given a set of decisions $\{d_i : j \in NB(i)\}$, node N_i adjusts initial decision $d_i \rightarrow z_i \in \{0, 1\}$ based on the majority voting strategy. In the end, all updated decisions z_i are communicated to the M2M GW, which again uses majority voting to make a decision based on z_i. Since LVDF is a corrected decision strategy, it can improve the sensing and processing reliability in M2M communications with additional information and temporal redundancy.

Reliability in Transmission

Consider that there are n total positive monitoring data on the same event in the M2M domain, and the M2M GW will report the decision to the BS only if it can collect more than k distinct monitoring data packets. For achieving communications efficiency, these positive monitoring data can first be aggregated and then forwarded to the GW together. However, in green M2M communications, not all nodes are active, which may result in unreliable transmission in the M2M domain. To improve transmission reliability, spatial redundancy technology can be adopted [7]. Specifically, each monitoring data packet is independently transmitted to the GW. Assume each transmission has equal transmission reliability p in the M2M domain, where $0 < p \leq 1$. Then the reliability of more than k out of n packets can reach the GW for making the correct decision, $\Sigma_{i=k}^{n} \binom{n}{k} p^i (1-p)^{n-i}$. Obviously, at the cost of redundant transmissions, the reliability in this strategy is higher than that in the aggregation transmission.

Reliability at the BS

After the M2M GW makes its decision on an event, it will forward the sensory and decisional data packet to the BS, and the BS will process these packets one by one in the application domain. In general, there is only one server activated to process these data packets for energy

In order to improve the reliability of M2M communications, exploiting redundancy technologies. including information redundancy, spatial redundancy and temporal redundancy, can be an efficient approach for M2M communications.

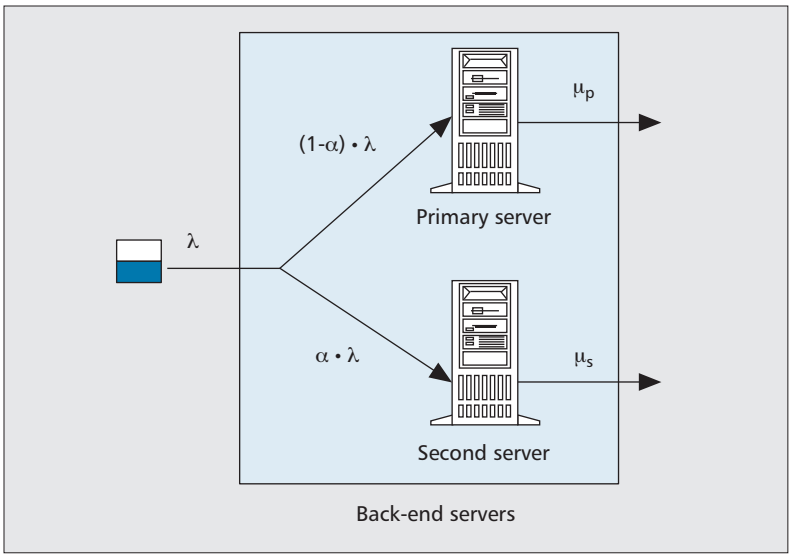

Figure 4. *The deployment of primary and second servers to achieve reliability.*

(power) saving purposes. However, when the number of arrival packets dramatically increases, especially during peak times, the single server cannot deal with the challenging situation, and reliability and QoS will degrade. To solve the reliability issue at the BS, a pair of servers, the primary server and second server, can be deployed at the application domain, as shown in Fig. 4. When the number of arrival packets is small, only the primary server is active; when the number of arrival packets is large, the second server will be active accordingly.

We model both the primary and second servers as M/M/1 queuing systems, where the means of service time are $1/\mu_p$ and $1/\mu_s$, respectively. Let λ be the arrival rate at the BS. If λ is small, all packets will be served by the primary server for energy saving. However, when λ increases, a fraction α, where $0 \le \alpha < \lambda$, of the packets will be served by the second server, and the rest, $1 - \alpha$ packets, will still be served by the primary server for guaranteeing the QoS in terms of average service delay. Therefore, the total average delay can be expressed as

$$E(D) = \frac{\alpha}{\mu_s - \lambda \cdot \alpha} + \frac{1-\alpha}{\mu_p - (1-\alpha)\lambda},$$

where $\mu_s - \lambda \cdot \alpha > 0$ and $\mu_p - (1 - \alpha)\lambda > 0$. By calculating the derivative

$$\frac{dE(D)}{d\alpha} = 0,$$

we have

$$\alpha = \frac{\sqrt{\mu_p}\mu_s - \sqrt{\mu_s}\mu_p + \sqrt{\mu_s}\lambda}{\left(\sqrt{\mu_p} + \sqrt{\mu_s}\right)\lambda}, \quad (1)$$

which indicates that

$$\lambda \le \mu_p - \sqrt{\mu_p \mu_s},$$

all packets are served by the primary server; when

$$\lambda > \mu_p - \sqrt{\mu_p \mu_s},$$

the second server will be adaptively active, and serve a fraction α of packets. Therefore, the reliability issues in M2M communications can be addressed by redundancy technologies; however, they will incur additional redundancy costs. How to balance greenness and reliability in M2M communications needs further exploration.

Security in M2M Communications

The research in security for M2M communications is still in its infancy. Security mainly targets the identification of potential attacks, threats, and vulnerabilities of M2M communications systems. In general, attacks in M2M can be classified as either passive or active. A passive attack does not disrupt the operations of an M2M communications system, but attempts to learn information about M2M communications by eavesdropping. Although difficult to detect, a passive attack causes less damage if well designed confidentiality mechanisms are adopted. In contrast, an active attack is easy to detect, but the damages are huge. An active attack is an attempt to deliberately modify sensory and decision data in the M2M and network domains, or gain authentication to access the BS in the application domain. In addition, active attacks can be further divided into external and internal attacks. An external attack is launched by attackers who are not equipped with key materials in an M2M communications system, while an internal attack is one from compromised M2M nodes that hold the key materials. Compared to the external attack, the internal attack obviously causes more serious damage to M2M communications systems.

Security Requirements for M2M Communication

To defend against the above security threats and establish a secure M2M communications environment, a suite of security mechanisms are desirable, which should achieve the following requirements:

Confidentiality: Confidentiality prevents unauthorized disclosure of sensory data in transmission from passive attackers, which ensures that only authorized entities can read these data in M2M communications systems.

Integrity: Integrity must be ensured so that illegal alteration of the sensory data (e.g., modifying, deleting, delaying, or replaying data) can be detected. In an M2M communications system, it is critical to meet the integrity requirement since illegal alteration may result in serious consequences, especially in life-critical M2M application contexts such as a remote e-healthcare system.

Authentication: Authentication is a prerequisite for secure M2M communications, allowing the BS in the application domain to corroborate the sensory data of the M2M nodes in the M2M domain.

Non-repudiation: Non-repudiation guarantees that M2M nodes, once sending data, cannot deny the transmission.

Access control: Access control is the ability to limit and control access to the BS in the application domain. Specifically, it allows only authorized M2M application systems to gain access to the BS.

Availability: Availability ensures that whenever M2M application systems access the BS, the BS is always available.

Privacy: Privacy is also of paramount importance in some privacy-sensitive M2M communications systems (e.g., e-healthcare systems). For example, if sensitive patient health information (PHI) is illegally disclosed or improperly used, e-healthcare systems can cause undesirably negative effects on patients' lives.

In general, the above security requirements in M2M communications can be achieved by cryptographic techniques. For example, symmetric or asymmetric encryption primitives can be employed to achieve confidentiality, and digital signature and message authentication code (MAC) techniques can achieve others. However, most security mechanisms only efficiently defend against external attacks. Once M2M nodes are compromised and launch some internal attacks in M2M communications, more sophisticated security mechanisms are needed.

Two Security Mechanisms Adapted to M2M Domain Security

In M2M communications systems, M2M nodes are generally deployed in the unattended M2M domain. They may be vulnerable to compromise attacks, and possibly launch different types of internal attacks controlled by the attacker. In the following, we introduce two sophisticated security mechanisms adapted to M2M domain security.

Early Detecting Node Compromise in M2M Domain — M2M node compromise attack is a serious threat to the success of M2M communications. Once M2M nodes are compromised, they can launch various internal attacks, such as false data injection, selective forwarding, wormhole and sybil attacks, to degrade the performance of an M2M communications system. Therefore, efficiently detecting the node compromise attack is very challenging in the M2M domain. When an attacker launches a node compromise attack, the attack process usually consists of three stages:

- *Stage 1*. The attacker physically captures and compromises the M2M nodes.
- *Stage 2*. The attacker redeploys the compromised M2M devices back into the M2M domain.
- *Stage 3*. The attacker controls the compromised nodes, rejoining the M2M domain and launching internal attacks.

Since the attacker usually requires some time to compromise the M2M nodes in stage 1, it is feasible for M2M nodes to form couples to monitor each other and detect node compromise early [8]. For example, as shown in Fig. 5a, shortly after M2M node deployment, either two neighboring M2M nodes form the H-node (husband node) and W-node (wife node), or three neighboring nodes form H-W-C nodes, where "C" represents the child node. Then both H-W nodes and H-W-C nodes can periodically monitor each other with beacon messages. Once an attacker physically compromises an M2M node, its beacon message becomes exceptional, and the couple nodes can detect a node compromise attack early. Therefore, couple detection builds the first line of defense against internal attacks in the M2M domain.

Bandwidth Efficient Cooperative Authentication to Filter False Reports in M2M Communications — To preserve energy, some M2M nodes switch to sleep mode. Then they could be compromised by an attacker without being detected. Later, these compromised nodes can inject false data and send them to the application domain, causing not only high-level erroneous decisions in an M2M application, but also energy wasted in multihop en route nodes. Since these compromised nodes hold key materials, pure cryptographic techniques are insufficient to defend against internal attack. To deal with this challenging issue, a bandwidth-efficient cooperative authentication (BECAN) scheme can be adopted [9]. As shown in Fig. 5b, to filter false data injected by compromised M2M nodes, BECAN applies the cooperative neighbor × router (CNR)-based filtering mechanism. Specifically, in the CNR-based mechanism, when an M2M node N_0 is ready to send sensory data m to the M2M GW via an established routing path $R_{N0}: [R_1 \rightarrow R_2 \rightarrow \cdots \rightarrow R_l \rightarrow GW]$, it first resorts to its k neighboring nodes $\{N_1, N_2, \cdots, N_k\}$ to cooperatively authenticate the sensory data m, and then sends the data m and the cooperation authentication information MAC to the GW via routing R_{N0}, where

$$MAC = \begin{bmatrix} mac_{01} & \cdots & mac_{0l} & mac_{0G} \\ mac_{11} & \cdots & mac_{1l} & mac_{1G} \\ mac_{21} & \cdots & mac_{2l} & mac_{2G} \\ \cdots & \cdots & \cdots & \cdots \\ mac_{k1} & \cdots & mac_{kl} & mac_{kG} \end{bmatrix}. \quad (2)$$

Each mac_{ij}, $0 \le i \le k$, $1 \le j \le l$, represents N_i's MAC on m for R_j's authentication, and each mac_{iG} represents N_i's MAC on m for the GW's authentication. When each M2M node is equipped with TinyECC-based public key materials (i.e., a pair of private and public key pair $(x_i, Y_i = x_iP)$), the non-interactive shared key $K_{ab} = x_aY_b = x_bYa = x_ax_bP$ between any N_a and N_b can be established. Then the full bipartite key graph between $N_0, N_1, N_2, \ldots, N_k$ and $R_1, R_2, \cdots, R_l, GW$ can be established, as shown in Fig. 5b. Because of the existence of a full bipartite key graph, the MAC design is reasonable. Therefore, when a compromised M2M node sends false data to the GW, the false data can be filtered if there is at least one uncompromised neighboring node participating in the reporting. To achieve bandwidth-efficient authentication, each mac_{ij} is compressed as 1 bit (i.e., $mac_{ij} = H(m||K_{ij}) \bmod 2$), and each mac_{iG} is compressed as α bits (i.e., $mac_{iG} = H(m||K_{iG}) \bmod 2^{\alpha}$), where $H()$ is a

In M2M communication systems, M2M nodes are generally deployed at unattended M2M domain. They may be vulnerable to the compromise attack, and possibly launch different types of internal attacks controlled by the attacker.

Although we have discussed the GRS issues in general M2M communications paradigm to shed light on this research line, further efforts are needed to identify the GRS issues in specific M2M communications contexts, e.g., a time-critical and privacy-sensitive eHealthcare system.

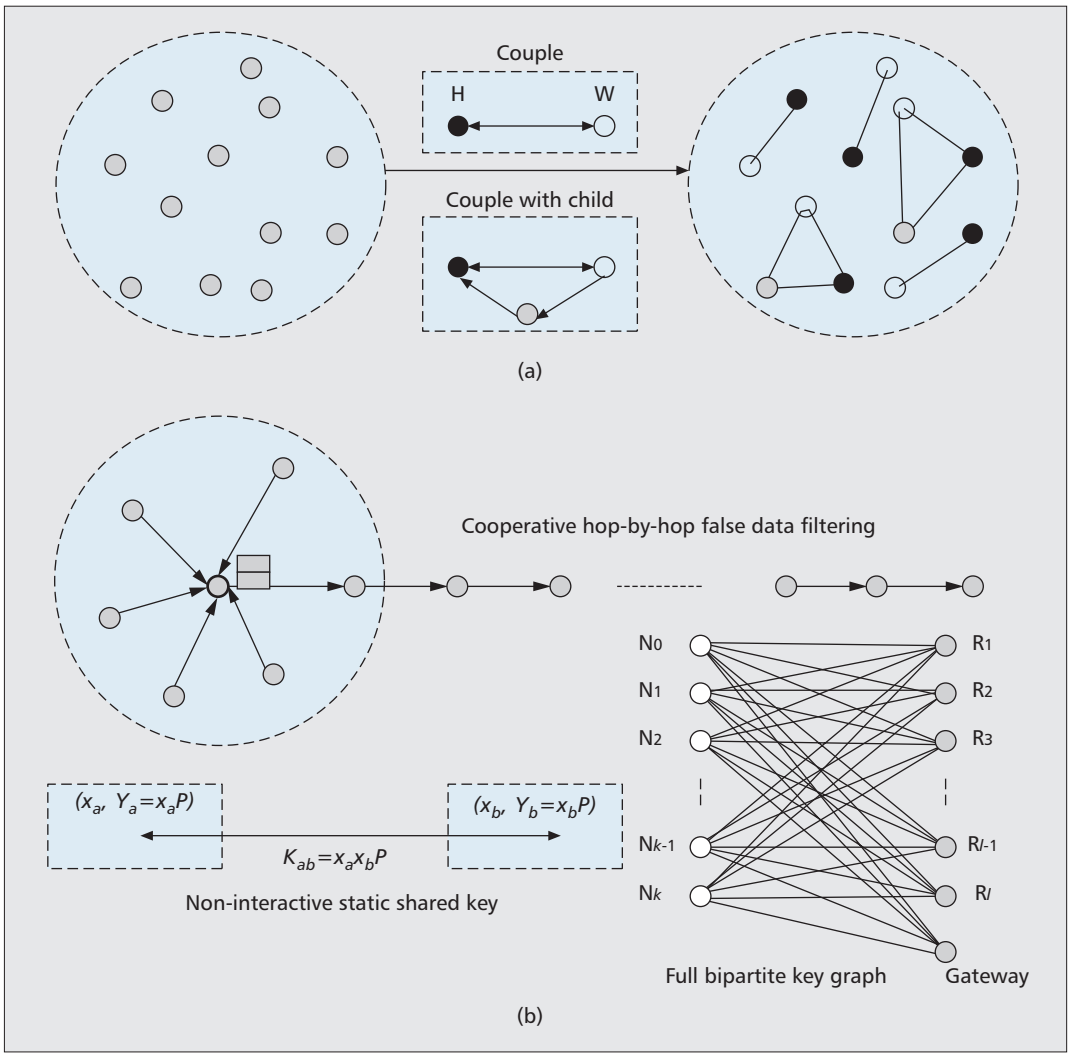

Figure 5. *Two security mechanisms adapted to M2M domain security: a) early detecting node compromise with couple; b) bandwidth-efficient cooperative authentication to filter false data.*

secure hash function and α is a security parameter. As a result, the scale of MAC is only $(1 + \alpha) \times (k + 1)$ bits.

To verify the efficiency of the BECAN, we conduct simulations where 1000 M2M nodes with transmission radius (TR) 15 m and 20 m are randomly deployed at a domain with 200 × 200 m^2, where each M2M node could be compromised with probability $\rho = 0.02$. The performance metrics used in simulation are en route filtering probability (EFP) and filtering ratio (FR) at each en route node, where EFP is defined as the fraction of the number of false data that are successfully filtered to the total number of injected false data; and FR at each en route node is defined as the fraction of the number of false data filtered at a specific en route node to the total number of filtered false data. Let the neighboring parameter $k = 4$; Fig. 6 shows the EFP in terms of different numbers of en route nodes. We can see that more than 90 percent EFP can be achieved, and as the number of en route nodes increases, EFP increases. In addition, EFP is lower with transmission radius 20 m than with 15 m. This is because the number of compromised neighboring nodes will increase when the transmission radius increases. Then a compromised M2M node has more chances to choose other neighboring compromised nodes participating in the attack to increase the attack's success probability. Therefore, parameter k and transmission radius should be well chosen in BECAN for better EFP. The inset in Fig. 6 shows the FR at each en route node. The results confirm the BECAN's effectiveness: false data can be detected early and filtered by the en route nodes, and the energy wasted in relaying injected false data can be reduced.

Conclusions

In this article, we have studied the issues to achieve green M2M communications by employing efficient activity scheduling techniques for energy saving. We have also offered several approaches to address the reliability and security issues in M2M communications. Although we have discussed the GRS issues in the general M2M communications paradigm to shed light on this research line, further efforts are needed to identify the GRS issues in specific M2M commu-

nications contexts (e.g., a time-critical and privacy-sensitive e-healthcare system [10]).

Acknowledgment

This research has been supported by a joint grant from the Natural Science and Engineering Research Council (NSERC) and Research In Motion (RIM), Canada.

References

[1] S. Gilani, "The Promise of M2M: How Pervasive Connected Machines are Fueling the Next Wireless Revolution," http://embedded-computing.com/white-machines-fueling-next-wireless-revolution, 2009.

[2] S. Hattangady, "Wireless M2M the Opportunity is Here! (Part 1)," http://emblazeworld.com/Attachments-Articles/2009-May Cellular Whitepaper Part 1.pdf

[3] R. Hodges and W. White, "Go Green in ICT," http://www.nascio.org/committees/green/whitepapers/bdna.pdf, 2008.

[4] A. Gallais *et al.*, "Localized Sensor Area Coverage With Low Communication Overhead," *IEEE Trans. Mobile Computing*, vol. 7, no. 5, 2008, pp. 661–72.

[5] I. Stojmenovic, "Localized Network Layer Protocols in Wireless Sensor Networks based on Optimizing Cost Over Progress Ratio," *IEEE Network*, vol. 20, no. 1, 2006, pp. 21–27.

[6] N. Katenka, E. Levina, and G. Michailidis, "Local Vote Decision Fusion for Target Detection in Wireless Sensor Networks," *IEEE Trans. Sig. Proc.*, vol. 56, no. 1, 2008, pp. 329–38.

[7] W. Lou *et al.*, "Spread: Improving Network Security by Multipath Routing in Mobile Ad Hoc Networks," *Wireless Networks*, vol. 15, no. 3, 2009, pp. 279–94.

[8] X. Lin, "CAT: Building Couples to Early Detect Node Compromise Attack in Wireless Sensor Networks," *Proc. IEEE GLOBECOM*, 2009, pp. 1–6.

[9] R. Lu *et al.*, "BECAN: A Bandwidth-Efficient Cooperative Authentication Scheme for Filtering Injected False Data in Wireless Sensor Networks," *IEEE Trans. Parallel and Distrib. Sys.*, 2010.

[10] X. Lin *et al.*, "SAGE: A Strong Privacy-Preserving Scheme against Global Eavesdropping for eHealth Systems," *IEEE JSAC*, vol. 27, no. 4, 2009, pp. 365–78.

Biographies

Rongxing Lu (rxlu@bbcr.uwaterloo.ca) [S'09, M'11] is currently working toward a Ph.D. degree with the Department of Electrical and Computer Engineering, University of Waterloo, Canada. He is currently a research assistant with the Broadband Communications Research (BBCR) Group, University of Waterloo. His research interests include wireless network security, applied cryptography, and trusted computing.

Xu Li (x279li@bbcr.uwaterloo.ca) received his Ph.D. degree from Carleton University, Canada, in October 2008, his Master's degree from the University of Ottawa, Canada, in May 2005, and his Bachelor's degree from Jilin University, China, in July 1998, all in computer science. He is currently an NSERC post-doc fellow with the BBCR Group, University of Waterloo. From 2008 to 2010, he worked as a post-doctoral researcher in INRIA, France, the University of Ottawa, Canada, and CNRS, France. His current research interests are in wireless ad hoc, sensor, and robot networks.

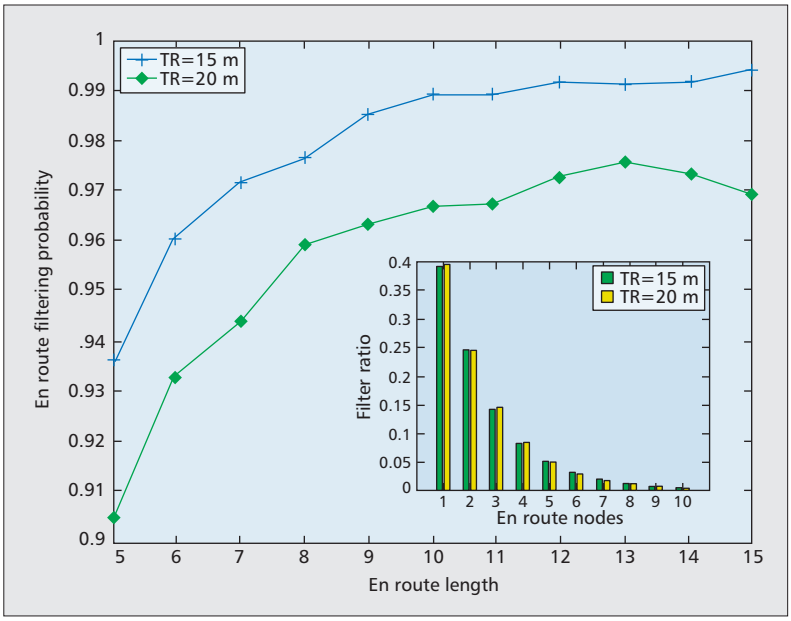

Figure 6. *Simulation results (EFP, FR) of BECAN for the neighboring parameter* k = *4, and the transmission radius* TR = *15, 20m.*

Xiaohui Liang (x27liang@bbcr.uwaterloo.ca) [S'10] is currently working toward a Ph.D. degree with the Department of Electrical and Computer Engineering, University of Waterloo, Canada. He is currently a research assistant with the Broadband Communications Research (BBCR) Group, University of Waterloo. His research interests include wireless network security, applied cryptography, and e-healthcare system.

Xiaodong Lin (xiaodong.lin@uoit.ca) [S'07, M'09] received a Ph.D. degree in information engineering from Beijing University of Posts and Telecommunications, China, in 1998 and a Ph.D. degree in electrical and computer engineering from the University of Waterloo in 2008. He is currently an assistant professor of information security with the Faculty of Business and Information Technology, University of Ontario Institute of Technology, Canada. His research interests include wireless network security, applied cryptography, computer forensics, and software security.

Xuemin (Sherman) Shen (xshen@bbcr.uwaterloo.ca) [M'97, SM'02, F'09] received a B.Sc. (1982) degree from Dalian Maritime University, China, and M.Sc. (1987) and Ph.D. degrees (1990) from Rutgers University, New Jersey, all in electrical engineering. He is a professor and University Research Chair, Department of Electrical and Computer Engineering, University of Waterloo. His research focuses on mobility and resource management, UWB wireless networks, wireless network security, and vehicular ad hoc and sensor networks. He served as an Area Editor for *IEEE Transactions on Wireless Communications* and Editor-in-Chief for *Peer-to-Peer Networks and Applications*. He is a Fellow of Engineering Institute of Canada, a registered Professional Engineer of Ontario, Canada, and a Distinguished Lecturer of the IEEE Communications Society.